Cours de mathématiques M.P.S.I.

D'après les cours de M. De Granrut

Henriet Quentin
Ausseil Lucas
Perard Arsène
Philipp Maxime

Nombres et structures algébriques usuelles

1. Nombres entiers naturels

1.1. Entiers naturels

$\mathbb{N}=\{0,1,2,...\}$
On connaît deux opérations : $+$, $\times$.

Définition :
Une loi de composition interne sur un ensemble E est une application :
$$* \ : \ \begin{matrix} E\times E\to E \\ (a,b)\mapsto a*b \end{matrix}$$

Exemple :
L'addition usuelle dans $\mathbb{N}$, $\mathbb{R}$, $\mathbb{C}$.

Propriétés éventuelles d'une loi de composition interne (LCI) :
- L'associativité : $\forall (a,b,c)\in E^3,\ a*(b*c)=(a*b)*c$ (ce qui autorise l'écriture $a*b*c$).
- La commutativité : $\forall (a,b)\in E^2,\ a*b=b*a$.
- Si $*$ et $+$ sont deux LCI sur E, on dit que $*$ est distributive par rapport à $+$ si :
$$\forall (a,b,c)\in E^3, \text{ on a : } \begin{cases} a*(b+c)=(a*b)+(a*c) \\ (b+c)*a=(b*a)+(c*a) \end{cases}$$

Définition :
Soit E un ensemble muni d'une LCI $*$ (on note $(E,*)$). $e\in E$ est dit neutre pour $*$ si :
$$\forall a\in E, a*e=e*a=a.$$

Remarques :
Un neutre n'existe pas toujours. S'il existe, il est unique.
Dans $\mathbb{N}$, 0 est le neutre de l'addition et 1 le neutre de la multiplication.

1.2. Relation d'ordre

Définition :
On appelle relation d'ordre sur E, une relation $\leqslant$ qui est :
- Réflexive : $\forall x\in E,\ x\leqslant x$
- Antisymétrique : $\forall x,y\in E,\ x\leqslant y$ et $y\leqslant x \ \Rightarrow \ x=y$
- Transitive : $\forall x,y,z\in E,\ x\leqslant y$ et $y\leqslant z \ \Rightarrow \ x\leqslant z$.

Exemple :
Dans $\mathbb{N}$ ou $\mathbb{R}$, $\leqslant$ est relation d'ordre mais pas $<$.

Définition :
Étant donné un ensemble ordonné $(E,\leqslant)$ et A une partie de E, on peut définir des éléments remarquables :
- $M\in E$ est un majorant de A si : $\forall x\in A, x\leqslant M \quad M\in E$
- $m\in E$ est un minorant de A si : $\forall x\in A, x\geqslant m \quad m\in E$
- $M\in A$ est le plus grand élément de A si : $\forall x\in A, x\leqslant M \quad M\in A$
- $m\in A$ est le plus petit élément de A si : $\forall x\in A, x\geqslant m \quad m\in A$

Remarque :
- Ces éléments n'existent pas toujours
- Le plus grand élément (le plus petit élément), quand il existe est unique.

Propriétés :

On admet les propriétés suivantes :

- Toute partie non vide de $\mathbb{N}$ possède un plus petit élément.
- Toute partie non vide et majorée de $\mathbb{N}$ possède un plus grand élément.
- Dans $\mathbb{N}$, $n<m \Rightarrow n \leqslant m-1$.

1.3. Principe de récurrence

Se reporter aux chapitres précédents.

→ Récurrence simple, sur deux rangs ou avec prédécesseurs.

→ Suites arithmétiques, géométriques.

1.4. Ensemble finis

Définition :

Un ensemble E est dit fini, s'il existe une bijection de $[\![1, n]\!]$ sur E. n est alors appelé cardinal de E.
On note $n=\text{Card}(E)$.

Remarque :

On admet que s'il existe une bijection de $[\![1, p]\!]$ sur $[\![1, n]\!]$, alors $n=p$.
Ce qui prouve l'unicité du cardinal.

Proposition :

Toute partie E' d'un ensemble fini E est finie et $\text{Card}(E') \leqslant \text{Card}(E)$ avec égalité si et seulement si $E'=E$.

Proposition :

Etant donnés deux ensembles finis E et F de même cardinal et $f : E \to F$
f est bijective si et seulement si f est injective ou surjective.

1.5. Dénombrement

Proposition :

Etant donnés E et F deux ensembles finis, si $n=\text{Card}(E)$ et $p=\text{Card}(F)$, on a :

1. $\text{Card}(E \cup F)=\text{Card}(E)+\text{Card}(F)-\text{Card}(E \cap F)$
2. $\text{Card}(\mathscr{F}(E, F))=p^n=\text{Card}(F^E)$
3. $\text{Card}(\mathscr{P}(E))=2^n$
4. Il y a $n!$ permutations dans E
5. Si $p \leqslant n$, il y a $n \times (n-1) \times \ldots \times (n-p+1)=\dfrac{n!}{(n-p)!}$ injections de F dans E
6. Si $p \leqslant n$, il y a $\binom{n}{p}$ parties à p éléments dans E.

2. Groupes et anneaux

2.1. Groupes

2.1.1. Symétriques

Définition :
Soit $(E,*)$ où $*$ est une LCI associative, possédant un élément neutre e.
$a\in E$ est dit symétrisable s'il existe $a'\in E$, appelé alors symétrique de a pour $*$, tel que : $a*a'=a'*a=e$.

Remarque :
Lorsqu'il existe, le symétrique d'un élément est unique.
En effet a' est un symétrique de a si : $a*a'=a'*a=e$
$a'*a*a''=(a'*a)*a''=a'*(a*a'')=e*a''=a'*e \Leftrightarrow a''=a'$.

Remarque :
Si x et y sont symétrisables alors $x*y$ est symétrisable et $(x*y)^{-1}=y^{-1}*x^{-1}$.

2.1.2. Définition

Définition :
Soit $(G,*)$ un ensemble muni d'une LCI. On dit que $(G,*)$ est un groupe si $*$ est une LCI associative, admettant un élément neutre et telle que tout élément de G est symétrisable.

Remarque :
Si la notation est additive $(G,+)$, le neutre de G est noté 0_G ou 0.
Si la notation est multiplicative $(G,\times)$, le neutre de G est noté 1_G ou 1.

Définition :
On dira qu'un groupe est commutatif (ou abélien) si $*$ est commutative.

Exemples :
$(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+),(\mathbb{C},+),(\mathbb{R}_+^*,\times),(\mathbb{R}^*,\times),(\mathbb{C}^*,\times),(\mathbb{U},\times),(\mathbb{U}_n,\times)$ sont des groupes (commutatifs).

Remarque :
$(\mathbb{N},+),(\{-1,0,1\},+),(\{-1,0,1\},\times)$ ne sont pas des groupes.

2.1.3. Sous-groupes

Définition :
Soit $(G,*)$ un groupe. Soit $H\subset G$. On dit que H est un sous-groupe de $(G,*)$ si H est une partie stable pour $*$ qui devient un groupe pour la loi (induite) $*$.

Remarque :
Le neutre de $(H,*)$ est le neutre de $(G,*)$.

Exemples :
$(\mathbb{Z},+)$ et $(\mathbb{R},+)$ sont des sous-groupes de $(\mathbb{C},+),(\mathbb{U},\times)$ et $(\mathbb{U}_n,\times)$ sont des sous-groupes de $(\mathbb{C},\times)$.

Remarque fondamentale :
Pour montrer qu'un ensemble G muni de la loi $*$ est un groupe, on reviendra rarement à la défintion : on cherchera plutôt un ensemble plus grand muni d'une extension de la loi qui est notoirement un groupe. On montrera alors simplement que $(G,*)$ est un sous-groupe à l'aide de l'un des deux théorèmes de caractérisation suivants :

Théorème :

Soient $(G,*)$ un groupe et $H \subset G$.

$(H,*)$ est un sous-groupe de $(G,*) \Leftrightarrow \begin{cases} 1. & H \neq \emptyset \\ 2. & \forall x \in H,\ x^{-1} \in H \\ 3. & \forall (x,y) \in H^2,\ x*y \in H \end{cases}$

Théorème :

Soient $(G,*)$ un groupe et $H \subset G$.

$(H,*)$ est un sous-groupe de $(G,*) \Leftrightarrow \begin{cases} 1. & H \neq \emptyset \\ 2. & \forall (x,y) \in H^2,\ x*y^{-1} \in H \end{cases}$

2.1.4. Morphismes de groupes

Définitions :

1. Soit $(G,*)$ et $(G',\top)$ deux groupes. Soit f une application de G dans G'. On dit que f est un morphisme de groupe si : $\forall (x,y) \in G^2,\ f(x*y) = f(x) \top f(y)$
2. Si de plus f est bijective, on dit que f est un isomorphisme (morphisme bijectif).
3. Si $f : G \to G$ alors f est un endomorphisme.
4. Un automorphisme est un endomorphisme bijectif.

Propriétés :

Si f est un morphisme de groupe, on a :

1. $f(e_G) = e_{G'}$
2. $\forall x \in G,\ f(x^{-1}) = [f(x)]^{-1}$
3. $\forall n \geqslant 1,\ \forall x \in G,\ f(x^n) = [f(x)]^n$

Preuve :

1. $f(e_G) = f(e_G * e_G) = f(e_G) \mathrm{T} f(e_G)$
   $\left(f(e_G)\right)^{-1} \mathrm{T} f(e_G) = \left(f(e_G)\right)^{-1} \mathrm{T} f(e_G) \mathrm{T} f(e_G)$
   $e_{G'} = e_{G'} \mathrm{T} f(e_G) = f(e_{G'} * e_G)$ donc $e_{G'} = f(e_G)$
2. $f(x) \mathrm{T} f(x^{-1}) = f(x * x^{-1}) = f(e_G) = e_{G'}$
   $f(x^{-1}) \mathrm{T} f(x) = f(x^{-1} * x) = f(e_G) = e_{G'}$
   Donc $\forall x \in G\ f(x^{-1}) = \left(f(x)\right)^{-1}$
3. Par récurrence : Pour $n=1$, $f(x^1) = \left(f(x)\right)^1$ Vraie
   On suppose $n \in \mathbb{N}^*$ et la formule vraie au rang n.
   $f(x^{n+1}) = f(x * x^n) = f(x) \top f(x^n) = f(x) \top \left(f(x)\right)^n = \left(f(x)\right)^{n+1}$
   Donc H_1 est vraie, et $H_n \Rightarrow H_{n+1}$.

Remarque :

On retrouve les propriétés de ln et exp à partir de leur équation fonctionnelle, et la formule de Moivre à partir de $\mathrm{e}^{i(\theta+\varphi)} = \mathrm{e}^{i\theta}\mathrm{e}^{i\varphi}$.

Proposition :

La composée de deux morphismes de groupes est un morphisme de groupes.
La fonction réciproque d'un isomorphisme est un isomorphisme de groupes (et aussi un isomorphisme).

Corollaire :

Soit $(G,*)$ un groupe. L'ensemble des automorphismes de G, noté $\mathrm{Aut}(G)$, est un groupe pour la loi $\circ$.

Définition :

On appelle noyau d'un isomorphisme f du groupe $(G,*)$ dans le groupe $(G',\top)$ et on note $\mathrm{Ker}(f)$:

$$\mathrm{Ker}(f) = f^{-1}(\{e_{G'}\}) = \{x \in G \text{ tel que } f(x) = e_{G'}\}.$$

Remarque :

En notation additive dans G', $\mathrm{Ker}(f)=f^{-1}(\{0_{G'}\})=\{x\in G \text{ tel que } f(x)=0_{G'}\}$.

En notation multiplicative dans G', $\mathrm{Ker}(f)=f^{-1}(\{1_{G'}\})=\{x\in G \text{ tel que } f(x)=1_{G'}\}$.

Proposition :

$\mathrm{Ker}(f)$ est un sous-groupe de G.

Preuve :

$\mathrm{Ker}(f)\subset G$

$f(e_{G'})=e_G \Rightarrow e_G\in\mathrm{Ker}(f) \Rightarrow \mathrm{Ker}(f)\neq\emptyset$

$\forall (x,y)\in\mathrm{Ker}(f),\ f(x*y^{-1})=f(x)\top f(y^{-1})=e_{G'}\top\left(f(y)\right)^{-1}=\left(e_{G'}\right)^{-1}=e_{G'} \Rightarrow x*y^{-1}\in\mathrm{Ker}(f)$

Donc $\mathrm{Ker}(f)$ est un sous-groupe de G.

Proposition fondamentale :

Soit f un morphisme de groupes.

f injective $\Leftrightarrow \mathrm{Ker}(f)=\{e_G\}$

Preuve :

$\Rightarrow$: $e_G\in\mathrm{Ker}(f)$ $\forall x\in\mathrm{Ker}(f),\ f(x)=e_{G'} \Leftrightarrow f(x)=f(e_G) \Leftrightarrow x=e_G$

$\Leftarrow$: $\forall x,y\in G,\ f(x)=f(y) \Rightarrow f(x)\otimes[f(y)]^{-1}=e_{G'} \Rightarrow f(x*y^{-1})=e_{G'} \Rightarrow x*y^{-1}\in\mathrm{Ker}(f)$

$\Rightarrow x*y^{-1}=e_G \Rightarrow x*y^{-1}*y=r_G*y \Rightarrow x=y$

Donc f injective.

Définition :

On appelle image d'un morphisime f du groupe $(G,*)$ dans le groupe $(G',\top)$ et on note $\mathrm{Im}(f)$:

$\mathrm{Im}(f)=f(G)=\{y\in G' \text{ tel que } \exists x\in G \text{ avec } f(x)=y\}=\{f(x), x\in G\}$.

Proposition :

$\mathrm{Im}(f)$ est un sous-groupe de G'.

Preuve :

$\cdot\ f(e_G)=e_{G'} \Rightarrow e_{G'}\in\mathrm{Im}(f) \Rightarrow \mathrm{Im}(f)\neq\emptyset$.

$\cdot\ \forall y\in\mathrm{Im}(f),\ \exists x\in G$ tel que $f(x)=y$ et on a : $f(x^{-1})=y^{-1} \Rightarrow y^{-1}\in\mathrm{Im}(f)$.

$\cdot\ \forall y_1,y_2\in\mathrm{Im}(f),\ \exists x_1,x_2\in G$ tels que $f(x_1)=y_1$ et $f(x_2)=x_2$ et on a :

$f(x_1*x_2)=y_1\top y_2 \Rightarrow y_1\top y_2\in\mathrm{Im}(f)$.

Remarque :

f est surjectif $\Leftrightarrow \mathrm{Im}(f)=G'$.

2.2. Anneaux

Définition :

Soient A un ensemble et $+$ et $\times$ deux LCI sur A. On dit que $(A,+,\times)$ est un anneau si :

1. $(A,+)$ est un groupe commutatif
2. $\times$ est associative, distributive par rapport à $+$
3. $\times$ admet un élément neutre noté 1_A(ou 1).

Remarque :

Le neutre de $+$ se note 0_A(ou 0) ; le symétrique de x pour $+$ se note $-x$.

Exemples :

$(\mathbb{Z},+,\times),(\mathbb{Q},+,\times),(\mathbb{R},+,\times),(\mathbb{C},+,\times),(\mathbb{K}[X],+,\times),(\mathcal{M}_2(\mathbb{R}),+,\times)$ sont des anneaux.

Définitions :

Soit $(A,+,\times)$ un anneau. On dit que :

$-$ A est commutatif si $\times$ est commutative.

$-$ A est intègre si $\forall (a,b)\in A,\ a\times b=0 \Rightarrow a=0$ ou $b=0$.

Exemple :

$\mathbb{Z},\mathbb{R},\mathbb{C},\mathbb{K}[X]$ sont intègres mais $(\mathcal{M}(\mathbb{K}),+,\times)$ n'est pas intègre.

Définition :

On appelle éléments inversibles d'un anneau $(A,+,\times)$ les éléments symétrisables pour $\times$ et on note :

$\mathbb{U}_A=\{\text{éléments inversibles de } (A,+,\times)\}$.

Proposition :

$(\mathbb{U}_A,\times)$ est un groupe.

Exemple :

$\mathbb{U}_{\mathbb{Z}}=\{-1,1\}, \mathbb{U}_{\mathbb{R}}=\mathbb{R}^*, \mathbb{U}_{\mathbb{K}[X]}=\mathbb{K}^*$.

Définition :

Soit $(A,+,\times)$ est un anneau et $B\subset A$. On dit que B est un sous-anneau de A si B est stable par $+$ et $\times$ et si $(B,+,\times)$ est un anneau pour les lois $+,\times$ (induites) avec $1_A=1_B$.

Théorème :

Soient $(A,+,\times)$ un anneau et $B\subset A$.

$(A,+,\times)$ est un sous-anneau de $A \Leftrightarrow \begin{cases} 1.\ \ 1_A\in B\ \ (\Rightarrow B\setminus\{0\}\neq\varnothing) \\ 2.\ \ \forall (b_1,b_2)\in B^2,\ \ b_1-b_2\in B \\ 3.\ \ \forall (b_1,b_2)\in B^2,\ \ b_1\times b_2\in B. \end{cases}$

Exemple :

$(\mathbb{Z},+,\times)$ est un sous-anneau de $(\mathbb{Q},+,\times)$.

Définition :

Soient $(A,+,\times)$ et $(B,+,\times)$ deux anneaux. On appelle morphisme d'anneau toute application $\varphi : A\to B$ telle que :

1. $\varphi(1_A)=1_B$
2. $\forall x,y\in A,\ \varphi(x+y)=\varphi(x)+\varphi(y)$
3. $\forall x,y\in A,\ \varphi(x\times y)=\varphi(x)\times\varphi(y)$.

* * * * *